UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/700,786	11/03/2003	Mariusz H. Jakubowski	MS1-1664US	5484

22801　　　7590　　05/21/2007	EXAMINER
LEE & HAYES PLLC	DEBNATH, SUMAN
421 W RIVERSIDE AVENUE SUITE 500	

	ART UNIT	PAPER NUMBER
SPOKANE, WA 99201	2135	

NOTIFICATION DATE	DELIVERY MODE
05/21/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

lhptoms@leehayes.com

	Application No.	Applicant(s)
Office Action Summary	10/700,786	JAKUBOWSKI ET AL.
	Examiner	Art Unit	
	Suman Debnath	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>19 April 2007</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-16,32-39 and 56-71</u> is/are pending in the application.

    4a) Of the above claim(s) <u>17-31, 40-55 and 72-85</u> is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-16, 32-39 & 56-71</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application

6)☐ Other: _____ .

DETAILED ACTION

1.   This written action is responding to the communication dated on 04/19/2007.

Election/Restrictions

2.   Applicant elected without traverse group I, claims 1-16, 32-39 and 56-71, in the
reply filed on April 19th, 2007.

3.   Claims 17-31, 40-55 and 72-85 corresponding to group 2 and group 3 are
withdrawn from further consideration as drawn to a non-elected invention.

Claim Objections

4.   Claims 1, 8, 15, 16, 70 and 71 are objected to for lack of antecedent basis:

Claim 1 recites "a user key" in line 5.

Claim 8 recites "each master key" in line 8.

Claim 15 recites "the selected user id" in line 17.

Claim 16 recites "the selected id" in line 6.

Claim 70 recites "the selected user id" in line 13.

Claim 71 recites "the selected user id" in line 7.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

5.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all
obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6.   Claims 1-6, 9-10, 32-36, 38-39 and 56-65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Challener et al. (Pub. No.: US 2003/0105980 A1), hereinafter "Challener" in view of Bailey (Patent No.: US 7,205,883 B2).

7.   As to claim 1, Challener discloses a method comprising: creating a data structure including a plurality of user id-user key pairs (FIG. 1, [0019]), each user id-user key pair comprising a user id associated with one of a plurality of users (FIG. 1, [0019], [0021]). Challener doesn't explicitly disclose a user key comprising a master key encrypted using a password associated with the one of the plurality of users; and delivering the data structure to one or more of the plurality of users.

However, Bailey discloses a user key comprising a master key encrypted using a password associated with the one of the plurality of users (FIG. 4, column 8, lines 7-25, "...the password retrieved from the host system is used to create a wrapping key K.........the SAK is wrapped using key K to produce a K-wrapped secondary authentication key..."); and delivering the data structure to one or more of the plurality of users (column 8, lines 7-25, "The [SAK].sub.K is transmitted to the host site...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to improve security in password-based access to a network.

8.   As to claims 32 and 56, these are rejected using the same rationale as for the rejection of claim 1.

9.   As to claim 57, it is rejected using the same rationale as for the rejection of claim 1.

10.   As to claims 2, 33, 58 and 59, Challener doesn't explicitly disclose wherein the act of delivering comprises delivering the data structure to each of the plurality of users. However, Bailey discloses wherein the act of delivering comprises delivering the data structure to each of the plurality of users (column 8, lines 7-25, "The [SAK].sub.K is transmitted to the host site...").

Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener as taught by Bailey in order to support multiple users in password-based access to a network.

11.·   As to claims 3 and 60, Challener discloses a hash of the password associated with the one of the plurality of users (FIG. 1, [0002]). Challener doesn't explicitly disclose wherein each master key is encrypted using a hash of the password. However, Bailey discloses wherein each master key is encrypted using a hash of the password (FIG. 4, column 8, lines 7-25).

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Challener as taught by Bailey

in order to improve security in password-based access to a network.

12.   As to claims 4, 5, 34, 35, 61 and 62, these are rejected using the same rationale

as for the rejection of claim 3.

13.   As to claims 6, 36 and 63, Challener discloses wherein each user key has an

integrity verification feature associated therewith ([0019], "The phrase signed with the

loaded private key is then compared with the stored signed phrase associated with the

remote user..").

14.   As to claims 9, 38 and 64, Challener discloses wherein each user key includes a

checksum ([0002], [0019]).

15.   As to claims 10, 39 and 65, Challener discloses wherein each user key includes

a keyed-hash message authentication code ([0019], "The phrase signed with the loaded

private key is then compared with the stored signed phrase associated with the remote

user..").

16.   Claims 7-8, 11-15, 37 and 66-70 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Challener in view of Bailey and further in view of Thomlinson et al.

(Patent No.: US 6,272,631 B1), hereinafter "Thomlinson".

17.   As to claims 7, 8 and 37, neither Challener nor Bailey explicitly discloses wherein

each master key has an integrity verification feature associated therewith. However,

Thomlinson discloses wherein each master key has an integrity verification feature

associated therewith (column 10, lines 30-65, "The master authentication key is used in

conjunction with the specified MAC to verity that the master key decrypted correctly").

        Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Challener and Bailey as taught by

Thomlinson in order to increase security by verifying the remote user's identity.

18.   As to claims 11 and 66, neither Challener nor Bailey explicitly discloses

transforming data using the master key. However, Thomlinson discloses transforming

data using the master key (column 10, lines 30-65, "The master key is then used to

decrypt an appropriate item key...").

        Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Challener and Bailey as taught by

Thomlinson in order to increase security by verifying the remote user's identity.

19.   As to claims 12 and 67, neither Challener nor Bailey explicitly disclose storing

data transformed using the master key; and controlling access by the plurality of users

to the transformed data. However, Thomlinson discloses storing data transformed using

the master key (column 9, lines 65-67, "The item key and item authentication key are

then encrypted using a master key"); and controlling access by the plurality of users to

the transformed data (column 9, lines 50-67 and column 10, lines 1-10).

        Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Challener and Bailey as taught by

Thomlinson in order to increase security by verifying the remote user's identity.

20.   As to claims 13 and 68, Challener discloses receiving a user id and user

password from one of the plurality of users ([0019], [0021]). Neither Challener nor Bailey

explicitly discloses storing data transformed using the master key; and controlling

access to the transformed data by the one of the plurality of users based on the

received user id and user password. However, Thomlinson discloses storing data

transformed using the master key (column 9, lines 50-67 and column 10, lines 1-10);

and controlling access to the transformed data by the one of the plurality of users based

on the received user id and user password (column 9, lines 30-67 and column 10, lines

1-10).

        Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Challener and Bailey as taught by

Thomlinson in order to increase security by verifying the remote user's identity.

21.   As to claims 14 and 69, these are rejected using the same rationale as for the

rejection of claim 13.

22.   As to claims 15 and 70, Challener discloses receiving a user id and user

password from one of the plurality of users ([0019], [0021]); selecting a user key from

the data structure based on the received user id (FIG. 1, [0019], [0021]). Challener

doesn't explicitly disclose storing data transformed using the master key; decrypting the

selected user id using the received password to reproduce the master key; and using

the master key to access the data.

    However, Bailey discloses decrypting the selected user id using the received

password to reproduce the master key (FIG. 4, column 8, lines 7-25, "..K-unwrapping of

[SAK].sub.K.").

    Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Challener as taught by Bailey

in order to improve security in password-based access to a network.

    Neither Challener nor Bailey explicitly discloses storing data transformed using

the master key; and using the master key to access the data.

    However, Thomlinson discloses storing data transformed using the master key

(column 9, lines 65-67, "The item key and item authentication key are then encrypted

using a master key"); and using the master key to access the data (column 9, lines 30-

67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time

of the invention was made to modify the teaching of Challener and Bailey as taught by

Thomlinson in order to increase security by verifying the remote user's identity.

23.   Claims 16 and 71 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Challener and further in view of Bailey, Thomlinson and Tewfik et al. (Pub. No.: US

2003/0095685 A1), hereinafter "Tewfik".

24.   As to claims 16 and 71, Challener discloses receiving a user id and user

password from one of the plurality of users ([0019], [0021]); selecting a user key from

the data structure based on the received user id (FIG. 1, [0019], [0021]). Hashing the

received password to produce a hash value (FIG. 1, [0002]). Challener doesn't explicitly

disclose storing data watermarked using the master key; decrypting the selected user id

using the received password to reproduce the master key; and using the master key to

access the watermarked data.

However, Bailey discloses decrypting the selected user id using the received

password to reproduce the master key (FIG. 4, column 8, lines 7-25, "..K-unwrapping of

[SAK].sub.K.").

Therefore, it would have been obvious to one of ordinary skill in the art at the

time of the invention was made to modify the teaching of Challener as taught by Bailey

in order to improve security in password-based access to a network.

Neither Challener nor Bailey explicitly discloses storing data watermarked using the master key; and using the master key to access the watermarked data.

However, Thomlinson discloses storing data transformed using the master key (column 9, lines 65-67, "The item key and item authentication key are then encrypted using a master key"); and using the master key to access the data (column 9, lines 30-67 and column 10, lines 1-10).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener and Bailey as taught by Thomlinson in order to increase security by verifying the remote user's identity.

Neither Challener and Bailey nor Thomlinson explicitly discloses watermarked data. However, Tewfik discloses watermarked data ([0015], [0020]). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention was made to modify the teaching of Challener, Bailey and Thomlinson as taught by Tewfik in order to protect contents from unauthorized duplication.

Conclusion

25.   The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See accompanying PTO 892.
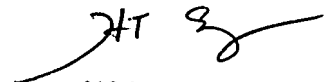
- US 6834112 B2 – Secure distribution of private keys to multiple clients.

- US 2002/0144128 A1 – Secure remote access and transmission.

26.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Suman Debnath whose telephone number is 571 270 1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

SD
LD

HOSUK SONG
PRIMARY EXAMINER